

In the Claims:

1. (Currently Amended) A method of generating an RSA cryptographic value, the method comprising the following carried out by hardware and/or software steps of:
obtaining user specific information about a user;
dividing a potential range of RSA prime values into at least two subintervals;
selecting a first user-dependent RSA prime from a range of RSA prime values in a first of the at least two subintervals corresponding to a user specific range of values based on the user specific information mapped onto the first subinterval; and
deriving an RSA key using the first user-dependent RSA prime.
2. (Previously Presented) A method according to Claim 1, further comprising the step of:
selecting a second user-dependent RSA prime from a range of RSA prime values in a second of the at least two subintervals, different from the first subinterval, corresponding to the user specific range of values based on the user specific information mapped onto the second subinterval.
3. (Original) A method according to Claim 1, wherein the user specific range of values are mapped by linearly mapping the user specific range of values onto the first subinterval.
4. (Original) A method according to Claim 2, wherein the user specific range of values are mapped onto the first subinterval and mapped onto the second subinterval utilizing the same mapping function.
5. (Original) A method according to Claim 2, further comprising the step of generating a user-dependent RSA key value from the first and second user-dependent primes.

6. (Original) A method according to Claim 1, wherein the RSA prime values comprise n bits and wherein the first subinterval comprises RSA prime values from the set $[\sqrt{2}(2^{n-1}), 2^{n-1} + 2^{n-3/2}]$ and the second subinterval comprises RSA prime values from the set $[2^{n-1} + 2^{n-3/2}, 2^n]$.

7. (Original) A method according to claim 2, wherein the RSA prime values comprise n bits and wherein the difference between the first RSA prime and the second RSA prime is greater than 2^{n-2} .

8. (Original) A method according to Claim 3, wherein the first subinterval comprises an interval [a,b], wherein the user specific range comprises an interval [c,d] and wherein the linear mapping function comprises the function defined by,

$$F(x) = ux + v, \text{ where } u = \frac{d - c}{b - a} \text{ and } v = \frac{bc - ad}{b - a}.$$

9. (Original) A method according to Claim 1 further comprising the step of selecting a second RSA prime from the potential range of RSA prime values.

10. (Original) A method according to Claim 1, wherein the user specific information is biometric information.

11. (Original) A method according to Claim 1, wherein the user specific information is a globally unique user identification.

12. (Previously Presented) A method according to Claim 1, wherein the step of selecting a first user-dependent RSA prime comprises the steps of:

selecting a random point in the range of RSA prime values in the first subinterval corresponding to the mapped user specific range of values; and

utilizing the random point as a starting point for a search for a prime number (p) in the

range of RSA prime values in the first subinterval corresponding to the mapped user specific range of values.

13. (Original) A method according to Claim 12, further comprising the steps of:

determining if a candidate for p is considered outside the range of RSA prime values in the first subinterval corresponding to the mapped user specific range of values;

selecting a new random point as a search starting point if a candidate for p is considered outside the range of RSA prime values in the first subinterval corresponding to the mapped user specific range of values; and

restarting the search for p utilizing the new random point.

14. (Currently Amended) A system for generating an RSA cryptographic value, comprising:

obtaining means for obtaining user specific information about a user;

determining means for determining a user specific range of values based on the user specific information;

dividing means for dividing a potential range of RSA prime values into at least two subintervals;

mapping means for mapping the user specific range of values onto a first of the at least two subintervals; ~~and~~

selecting means for selecting a first user-dependent RSA prime from the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values; and

deriving means for deriving an RSA key using the first user-dependent RSA prime.

15. (Currently Amended) A system according to Claim 14, wherein the mapping means comprises first mapping means, the system further comprising:

second mapping means for mapping the user specific range of values onto a second of the at least two subintervals, different from the first of the at least two subintervals;

selection means for selecting a second user-dependent RSA prime from the range of RSA prime values in the second of the at least two subintervals corresponding to the mapped user specific range of values.

16. (Currently Amended) A system according to Claim 15, wherein the first mapping means for mapping comprises linear mapping means for linearly mapping the user specific range of values onto a first of the at least two subintervals.

17. (Currently Amended) A system according to Claim 16, wherein the first mapping means for mapping the user specific range of values onto a first of the at least two subintervals and the second mapping means for mapping the user specific range of values onto a second of the at least two subintervals, different from the first of the at least two subintervals utilize the same mapping function.

18. (Currently amended) A system according to Claim 15, wherein the deriving means for deriving an RSA key using the first user-dependent RSA prime further comprises generating means for generating a user-dependent RSA key value from the first and second user-dependent primes.

19. (Original) A system according to Claim 14, wherein the RSA prime values comprise n bits and wherein the first subinterval comprises RSA prime values from the set $[\sqrt{2}(2^{n-1}), 2^{n-1} + 2^{n-3/2}]$ and the second subinterval comprises RSA prime values from the set $[2^{n-1} + 2^{n-3/2}, 2^n]$.

20. (Original) A system according to claim 15, wherein the RSA prime values comprise n bits and wherein the difference between the first RSA prime and the second RSA prime is greater than 2^{n-2} .

21. (Original) A system according to Claim 16, wherein the first subinterval comprises an interval [a,b], wherein the user specific range comprises an interval [c,d] and wherein the linear mapping function comprises the function defined by,

$$F(x) = ux + v, \text{ where } u = \frac{d - c}{b - a} \text{ and } v = \frac{bc - ad}{b - a}.$$

22. (Currently Amended) A system according to Claim 14 further comprising selection means for selecting a second RSA prime from the potential range of RSA prime values.

23. (Original) A system according to Claim 14, wherein the user specific information is biometric information.

24. (Original) A system according to Claim 14, wherein the user specific information is a globally unique user identification.

25. (Currently Amended) A system according to Claim 14, wherein the selecting means for selecting a first user-dependent RSA prime comprises:

selection means for selecting a random point in the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values;

searching means for utilizing the random point as a starting point for a search for a prime number (p) in the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values.

26. (Currently Amended) A system according to Claim 25, further comprising:
determining means for determining if a candidate for p is considered outside the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped

user specific range of values;

selection means for selecting a new random point as a search starting point if a candidate for p is considered outside the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values; and

restarting means for restarting the search for p utilizing the new random point.

27. (Currently Amended) A computer program product for generating an RSA cryptographic value, comprising:

a computer readable storage medium having computer readable program code ~~means~~ embodied in said medium, said computer readable program code means comprising:

first computer-readable program code ~~means for obtaining that is configured to obtain~~ user specific information about a user;

second computer-readable program code ~~means for determining that is configured to determine~~ a user specific range of values based on the user specific information;

third computer-readable program code ~~means for dividing that is configured to divide~~ a potential range of RSA prime values into at least two subintervals;

fourth computer-readable program code ~~means for mapping that is configured to map~~ the user specific range of values onto a first of the at least two subintervals; and

fifth computer-readable program code ~~means for selecting that is configured to select~~ a first user-dependent RSA prime from the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values; and

sixth computer-readable program code ~~means for deriving that is configured to derive~~ an RSA key using the first user-dependent RSA prime.

28. (Currently Amended) A computer program product according to Claim 27, further comprising:

seventh computer-readable program code ~~means for mapping that is configured to map~~ the user specific range of values onto a second of the at least two subintervals, different from the first of the at least two subintervals; and

eighth computer-readable program code means ~~for selecting that is configured to select~~ a second user-dependent RSA prime from the range of RSA prime values in the second of the at least two subintervals corresponding to the mapped user specific range of values.

29. (Currently Amended) A computer program product according to Claim 28, wherein the seventh computer-readable program code ~~means for mapping~~ comprises ninth computer-readable program code ~~means for that is configured to linearly mapping map~~ the user specific range of values onto a first of the at least two subintervals.

30. (Currently Amended) A computer program product according to Claim 29, wherein the fourth computer-readable program code ~~means for mapping the user specific range of values onto a first of the at least two subintervals~~ and the seventh computer-readable program code ~~means for mapping the user specific range of values onto a second of the at least two subintervals, different from the first of the at least two subintervals~~ utilize the same mapping function.

31. (Currently Amended) A computer program product according to Claim 28, wherein the sixth computer-readable program code ~~means for deriving an RSA key using the first user dependent RSA prime~~ further comprises ninth computer readable program code ~~means for generating that is configured to generate~~ a user-dependent RSA key value from the first and second user-dependent primes.

32. (Original) A computer program product according to Claim 26, wherein the RSA prime values comprise n bits and wherein the first subinterval comprises RSA prime values from the set $[\sqrt{2}(2^{n-1}), 2^{n-1} + 2^{n-3/2}]$ and the second subinterval comprises RSA prime values from the set $[2^{n-1} + 2^{n-3/2}, 2^n]$.

33. (Original) A computer program product according to claim 28, wherein the RSA prime values comprise n bits and wherein the difference between the first RSA prime and the second RSA prime is greater than 2^{n-2} .

34. (Original) A computer program product according to Claim 29, wherein the first subinterval comprises an interval [a,b], wherein the user specific range comprises an interval [c,d] and wherein the linear mapping function comprises the function defined by,

$$F(x) = ux + v, \text{ where } u = \frac{d - c}{b - a} \text{ and } v = \frac{bc - ad}{b - a}.$$

35. (Currently Amended) A computer program product according to Claim 27 further comprising seventh computer-readable program code ~~means for selecting that is configured to select~~ a second RSA prime from the potential range of RSA prime values.

36. (Original) A computer program product according to Claim 27, wherein the user specific information is biometric information.

37. (Original) A computer program product according to Claim 27, wherein the user specific information is a globally unique user identification.

38. (Currently Amended) A computer program product according to Claim 27, wherein the fifth computer-readable program code ~~means for selecting a first user dependent RSA prime~~ comprises:

seventh computer-readable program code ~~means for selecting that is configured to select~~ a random point in the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values; and

eighth computer-readable program code ~~means for utilizing that is configured to utilize~~ the random point as a starting point for a search for a prime number (p) in the range of

RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values.

39. (Currently Amended) A computer program product according to Claim 38, further comprising:

ninth computer-readable program code ~~means for determining that is configured to determine~~ if a candidate for p is considered outside the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values;

tenth computer-readable program code ~~means for selecting that is configured to select~~ a new random point as a search starting point if a candidate for p is considered outside the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values; and

eleventh computer-readable program code ~~means for restarting that is configured to restart~~ the search for p utilizing the new random point.

40. (Currently Amended) A method of generating a cryptographic value corresponding to a source entity, the method comprising the following carried out by hardware and/or software steps of:

obtaining entity specific information associated with the source entity; ~~and~~
selecting a cryptographic value from a range of cryptographic values based on the entity specific information, wherein the range of cryptographic values based on the entity specific information is disjoint with ranges of cryptographic values associated with entity specific information associated with entities other than the source entity; and
deriving a cryptographic key value based on the selected cryptographic value.

41. (Original) A method according to Claim 40, wherein the entity specific information comprises biometric information associated with a user.

42. (Original) A method according to Claim 40, wherein the entity specific information comprises a globally unique user identification associated with a user.

43. (Original) A method according to Claim 40, wherein the entity specific information comprises a company identification.

44. (Currently Amended) A method according to Claim 40, wherein the cryptographic value comprises an RSA key and wherein the step of selecting comprises selecting the RSA key from a portion of the range of potential RSA key values based on the entity specific information, wherein portion of the range of potential RSA key values is defined by mapping an entity specific range of values onto the range of potential key values and wherein the step of deriving a cryptographic key value based on the selected cryptographic value comprises providing the selected RSA key as the derived cryptographic key value.

45. (Original) A method according to Claim 40, further comprising the step of authenticating the source entity of the cryptographic value by determining if the cryptographic value is within the range of cryptographic values based on the entity specific information associated with the source entity.

46. (Currently Amended) A system for generating a cryptographic value corresponding to a source entity, comprising:

obtaining means for obtaining entity specific information associated with the source entity;

selecting means for selecting a cryptographic value from a range of cryptographic values based on the entity specific information, wherein the range of cryptographic values based on the entity specific information is disjoint with ranges of cryptographic values associated with entity specific information associated with entities other than the source entity; and

deriving means for deriving a cryptographic key value based on the selected cryptographic value.

47. (Original) A system according to Claim 46, wherein the entity specific information comprises biometric information associated with a user.

48. (Original) A system according to Claim 46, wherein the entity specific information comprises a globally unique user identification associated with a user.

49. (Original) A system according to Claim 46, wherein the entity specific information comprises a company identification.

50. (Currently Amended) A system according to Claim 46, wherein the cryptographic value comprises an RSA key and wherein the selecting means for selecting comprises selection means for selecting the RSA key from a portion of the range of potential RSA key values based on the entity specific information, wherein portion of the range of potential RSA key values is defined by mapping an entity specific range of values onto the range of potential key values and wherein the deriving means for deriving a cryptographic key value based on the selected cryptographic value comprises providing means for providing the selected RSA key as the derived cryptographic key value.

51. (Currently Amended) A system according to Claim 46, further comprising authentication means for authenticating the source entity of the cryptographic value by determining if the cryptographic value is within the range of cryptographic values based on the entity specific information associated with the source entity.

52. (Currently Amended) A computer program product for generating a cryptographic value corresponding to a source entity, comprising:

a computer readable storage medium having computer readable program code means embodied in said medium, said computer readable program code means comprising:

first computer readable program code ~~means for obtaining that is configured to obtain~~ entity specific information associated with the source entity;

second computer readable program code ~~means for selecting that is configured to select~~ a cryptographic value from a range of cryptographic values based on the entity specific information, wherein the range of cryptographic values based on the entity specific information is disjoint with ranges of cryptographic values associated with entity specific information associated with entities other than the source entity; and

third computer readable program code ~~means for deriving that is configured to derive~~ a cryptographic key value based on the selected cryptographic value.

53. (Original) A computer program product according to Claim 52, wherein the entity specific information comprises biometric information associated with a user.

54. (Original) A computer program product according to Claim 52, wherein the entity specific information comprises a globally unique user identification associated with a user.

55. (Original) A computer program product according to Claim 52, wherein the entity specific information comprises a company identification.

56. (Currently Amended) A computer program product according to Claim 52, wherein the cryptographic value comprises an RSA key and wherein the second computer readable program code ~~means for selecting~~ comprises fourth computer readable program code ~~means for selecting that is configured to select~~ the RSA key from a portion of the range of potential RSA key values based on the entity specific information, wherein portion of the range of potential RSA key values is defined by mapping an entity specific range of values onto the range of potential key values and wherein the third computer readable program code

In re: Matyas, Jr. et al.
Serial No.: 09/324,308
Filed: June 2, 1999
Page 14 of 18

~~means for deriving a cryptographic key value based on the selected cryptographic value~~
comprises fifth computer readable program code ~~means for providing that is configured to~~
provided the selected RSA key as the derived cryptographic key value.

57. (Currently Amended) A computer program product according to Claim 52, further comprising fourth computer readable program code ~~means for authenticating~~ configured to authenticate the source entity of the cryptographic value by determining if the cryptographic value is within the range of cryptographic values based on the entity specific information associated with the source entity.